Penn State Journal of Law & International Affairs

Volume 5
Issue 1 *War in the 21st Century and Collected Works*

April 2017

Maintaining Individual Liability in AML and Cybersecurity at New York's Financial Institutions

Harry Dixon

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

MAINTAINING INDIVIDUAL LIABILITY IN AML AND CYBERSECURITY AT NEW YORK'S FINANCIAL INSTITUTIONS

*Harry Dixon**

Cybersecurity in the financial sector is of paramount importance. Due to significant cyber intrusions affecting some of the world's biggest banks, in September 2016 New York's Department of Financial Services ("NYDFS") proposed regulations requiring banks and insurance companies to establish cybersecurity programs and designate an internal cybersecurity officer. These rules became final in March 2017. Described as a "first-in-the-nation" effort, the regulations will only affect banks and other financial services providers in New York. However, given New York's outsized influence on the financial services industry, it is likely that this will set a precedent for both state and federal regulators. Thus, NYDFS would do well to set a good precedent.

Unfortunately, at least some of the rules need serious improvement. In particular, the proposed regulations require that either the chairperson of the board or a senior officer certify that the firm's cybersecurity program meets the proposal's requirements. Those submitting the certification could be held individually liable if the organization's cybersecurity program is deficient. This liability includes civil and criminal penalties.

However, this contrasts with NYDFS's rule regarding anti-money laundering ("AML") and Office of Foreign Assets Control ("OFAC") transaction monitoring and filtering programs. Under those rules, there are no criminal penalties for individual directors. Because recent developments in financial institutions suggest that AML policy and cybersecurity policy are significantly intertwined and are not easily separable; to track consistency with developments in federal law pertaining to individual liability in corporations; and to maintain consistency and clarity in the law, the NYDFS should, where appropriate, allow its regulators to pursue criminal liability against individuals.

* Associate, Taylor English Duma LLP, Atlanta, Georgia
University of Georgia, Honors Program 2007 - B.B.A. Economics, *cum laude*,(honors); B.A. History, *cum laude* (honors); University of Georgia School of Law, 2013, Juris Doctor (J.D); and, Certified Anti-Money Laundering Specialist (CAMS). The author would like to thank his family and friends for their support, as well as Cam Piasecki for his commentary and revisions.

TABLE OF CONTENTS

I. INTRODUCTION

Everyday hackers attack financial institutions for a variety of motives. Some hackers target financial institutions for money, others, for "the lulz." Still, others hack financial institutions for political motivations because by doing so, they may cause damage to the global economy.

In any of these scenarios the potential for damage is significant. For example, in 2013 a Kiev ATM began randomly dispensing money throughout the day.[1] When a Russian cybersecurity firm began to investigate, they discovered that the ATM was only the tip of the iceberg: malware had severely penetrated the bank's computers, even sending back video feeds of employees conducting routine tasks throughout the day.[2] The criminal group – comprised of Chinese, Russians, and Europeans – were then able to impersonate bank officers, turn on various cash machines, and transfer millions of dollars from banks throughout the world into dummy accounts.[3]

The largest financial institution hack in U.S. history highlights the damages a hack can cause. The United States Attorney's Office for the Southern District of New York charged Gery Shalon, Joshua Samuel Aron, and Ziv Orenstein in a 23-count indictment in November of 2015.[4] In addition to charging the men with securities fraud and money laundering, the indictment alleged that the men had stolen the personal information of more than 100 million customers.[5] As these examples demonstrate, cybersecurity in the financial sector is of paramount importance.

Due to these attacks, along with other significant cyber intrusions affecting some of the world's biggest banks, the New

---

[1] David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N.Y. TIMES (Feb. 14, 2015), *available at* http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

[2] *Id.*

[3] *Id.*

[4] U.S. v. Shalon, Aaron, and Orenstein, No. 15-cr-333 (S.D. N.Y. 2015).

[5] *Id.*

York's Department of Financial Services [*hereinafter* "NYDFS"] proposed regulations[6] requiring banks and insurance companies to establish cybersecurity programs and designate an internal cybersecurity officer in September of 2016.[7] These regulations were the result of years of research that probed weaknesses in financial institutions and then asked for feedback from those institutions regarding their efforts to strengthen their cybersecurity regimes. The results established the groundwork for the basic regulations, subject to a public comment period that closed in November of 2016. The rules became effective on March 1st, 2017.

Described as a "first-in-the-nation" effort,[8] the regulations will only affect banks and other financial services providers in New York; nevertheless, *only* is a relative term. Given New York's outsized influence on the financial services industry the rules will set a precedent for cybersecurity within financial institutions, and, both state and federal regulators may use the rules as a framework for their own cybersecurity rules and regulations. Thus, it is important that the NYDFS set a rigorous, clear standard that reflects reality and assesses liability where appropriate.

Unfortunately, the NYDFS has unintentionally created a conflict amongst their rules. The cybersecurity regulations require either the chairperson of the board or a senior officer certify the firm's cybersecurity program meets the proposal's requirements in an annual certification.[9] Those submitting the certification can be held

---

[6] Hereinafter, unless specified otherwise, the terms "regulations" or "the regulations" should be assumed to be referring to the DFS's proposed regulations discussed here.

[7] Sanger & Pelroth, *supra* note 2.

[8] Governor Cuomo, Press Release, *Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions*, OFFICIAL NEWS FROM THE OFFICE OF THE GOVERNOR (September 13, 2016), *available at* https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-first-nation-cybersecurity-regulation-protect-consumers-and [*hereinafter* "Governor Cuomo Press Release"].

[9] 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies, N.Y. DEP'T FIN. SERVS., Section 500.00 (Feb. 2017), *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf.

individually liable if the organization's cybersecurity program is deficient.[10] This liability includes civil and criminal penalties.[11] Such a program is often standard in today's corporate culture.

This rule conflicts with NYDFS's rule regarding anti-money laundering [*hereinafter* "AML"] and Office of Foreign Assets Control [*hereinafter* "OFAC"] transaction monitoring and filtering programs. Under the AML and OFAC rules, there are no explicit criminal penalties for individual directors, nor is there an annual certification procedure.[12] As it follows, a situation could arise where a director would not be liable under the AML rule, but would be liable under the cybersecurity rule.

While such a discrepancy in the rules may not seem important, in the context of financial institutions, data breaches and money laundering often go hand-in-hand, as demonstrated by the above example. Indeed, given the broad scope of money laundering laws, money laundering is almost guaranteed to occur in a data breach of a financial institution, even if the theft only amounts to a penny. But that is not the only reason why cybersecurity and AML rules regarding certification should harmonize. Recent developments in U.S. corporate liability law at the federal level may very well influence individual corporate liability at the state level. Thus, the NYDFS should, where appropriate, allow its regulators to pursue criminal liability on both individuals, and the corporation. This will create clarity in the law; reflect the reality of intertwined AML and cybersecurity policies and close a loophole; and will track federal legal developments.

Part II of this article will briefly explain the background of modern individual corporate liability, cybersecurity, and money laundering. In Part III, the proposed rules will be examined and

---

[10] *Id.* at 500.20.

[11] *Id.* at 500.20.

[12] *See generally NYDFS Issues Final Anti-Money Laundering and Sanctions Rule*, DEBEVOISE PLIMPTON (Jul. 6, 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/07/20160706_nydfs_issues_final_anti_money_laundering_and_sanctions_rule.pdf (discussing final changes to AML rule, including removal of compliance rule and threat of criminal penalties).

explained. As we will see, AML and cybersecurity are so intertwined that it does not make sense to have different standards for what is quickly becoming the same group. In Part IV, this author will propose a modification in accordance with New York corporate liability law that reflects the reality of AML and cybersecurity policy. Part V, consists of the author's closing remarks.

II. BACKGROUND

A. Corporate criminal liability for individuals

New York is the birthplace of corporate criminal liability. In *New York Central & Hudson River Railroad v. United States*,[13] the question before the U.S. Supreme Court was whether Congress had acted constitutionally when, via the Elkins Act, legislators imputed criminal liability to a common carrier where any agents and officers of a common carrier granted an illegal rebate.[14] The Court held that Congress could subject a corporation to criminal punishment solely on the basis of an agent's conduct because the Court saw "no valid objection in law, and every reason in public policy, why the corporation which profits by the transaction, and can only act through its agents and officers, shall be held punishable."[15]

Corporate criminal liability law has existed in some capacity in New York since at least 1948.[16] In those days, the state of New York imposed a $5,000 fine for a corporation convicted of a felony that would lead to imprisonment.[17] At the time, case law suggested that

---

[13] New York Central R Co. v. United States, 212 U.S. 481 (1909). For an excellent discussion of this case and modern corporate criminal liability, *see* Andrew Weissmann with David Newman, *Rethinking Criminal Corporate Liability*, 82 INDIANA L. J. 411, 420-421 (2013) (discussing *New York Central*).

[14] *Id.* at 421.

[15] *N.Y. Cent.*, 212 U.S. at 495.

[16] *See Corporate Criminal Liability in New York*, 48 COLUM. L. REV. 794 (1948) ("under the present state of law, a corporation may be liable for almost any crime perpetrated in connection with corporate activities.").

[17] *Id.* at 794.

directors, officers, or employees acting within the scope of their authority could render a corporation criminally liable.[18]

It was around this time that a theory began to form of holding individuals in corporations accountable for crimes. During the Nuremberg trials after World War II, Justice Robert Jackson, Chief Counsel for the United States at Nuremberg, stated during the trial of industrialist Gustav Krupp that, "the great industrialists of Germany were guilty of the crimes charged in this indictment quite as much as its politicians, diplomats, and soldiers."[19] Other cases followed involving industrialists committing war crimes through their corporations.[20] Still, with the exception of acts constituting war crimes,[21] or blatant statutory violations such as securities fraud, for decades prosecuting individuals for crimes committed in connection with their work at a corporation was uncommon.

H. David Kotz, former Inspector General at the Securities and Exchange Commission and current Managing Director of the Berkeley Research Group, has two theories on why this has occurred. First, historically, companies were much more likely to engage in a settlement process with the government, whereas individuals who faced prison time were much more likely to fight any charges. A recalcitrant individual is not preferable to a prosecutor, who unfortunately tends to be overworked and is trying to resolve a case

---

[18] *Id.* at 795 (*citing*, e.g., People v. Lawyers Title Corp., 282 N.Y. 513, 27 N.E. 2d 30 (1940) (illegal practice of law); People v. Woodbury Dermatological Institute, 192 N.Y. 454, 85 N.E. 697 (1908) (illegal practice of medicine); People v. Globe Jewelers Inc. 249 App. Div. 122, 291 N.Y. Supp. 362 (1st Dep't 1936) (treasurer of the corporation sent out a fake form, simulating a court order)) (footnote omitted).

[19] Chatham House, *What Are the Relevant Legal Principles Relating to the Responsibility of Companies and CEOs for Violations of International Criminal Law?* (2012).

[20] *Id.*

[21] *See* Rule 156, Definition of War Crimes, Int'l. Comm. Of Red Cross (defined as "serious violations of the laws and customs applicable in international armed conflict" and "serious violations of the laws and customs applicable in an armed conflict not of an international character,"), https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule156 (last visited Mar. 30, 2017).

as quickly as possible.[22] Secondly, and on a related note, corporations do not face the negligence or intent requirement that individuals face in criminal prosecutions, nor is there a priority for cases that are novel, challenging, and difficult to prove, which shifted enforcement away from individuals and instead towards more obvious corporate conduct with a lower evidentiary threshold.[23]

Yet, because of a flurry of disastrous financial events ranging from Enron's collapse to the financial meltdown of 2008, the enforcement approach utilized by agencies has changed dramatically in the past decade. For years critics argued that the Department of Justice [*hereinafter* "DOJ"] and the Securities and Exchange Commission [*hereinafter* "SEC"] were not doing much to bring civil and criminal cases against parties involved in the 2008 financial crisis.[24] For example, in 2013 Jed Rakoff, U.S. District Court Judge of the Southern District of New York – no stranger to fraud trials prosecuted by the SEC –, complained that the government was not holding individuals responsible for massive frauds, "speak[ing] greatly to weaknesses in our prosecutorial system."[25]

This sentiment set the stage for a memorandum from Deputy Attorney General Sally Yates in September 2015 that outlines a new DOJ policy regarding individual liability in corporate contexts, which came to be known as the "Yates Memo."[26] Since the memo, the DOJ has increasingly imposed criminal and civil liability for individuals conducting corporate misconduct.[27] This policy also requires

---

[22] Berkeley Research Paper, https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/white-paper/yates-memo-background-and-its-impact-white-paper.pdf (registration required).

[23] *Id.*

[24] *Id.*

[25] *Id.* (*quoting* Nate Raymond, *Judge Criticizes Lack of Prosecution against Wall Street Executives for Fraud*, REUTERS (Nov. 12, 2013), http://www.reuters.com/article/financial-judge-idUSL2N0IX1B620131113.

[26] Individual Accountability for Corporate Wrongdoing, Sally Q. Yates, Department of Justice, Sept. 9, 2015, https://www.justice.gov/dag/file/769036/download.

[27] Roberto J. Gonzalez & Jessica S. Carey, *The Government's Making AML Enforcement Personal*, NAT'L L. J. (Feb. 22, 2016), *available at* https://www.paulweiss.com/media/3359752/gonzalez_carey__nlj_022216.pdf.

companies to provide "all" relevant facts about "all" individuals involved in wrong doing, regardless of "position, status, or seniority," in order for the company to get any kind of cooperation credit.[28]

The election of President Donald J. Trump makes it unclear whether the Yates memo will continue to be enforced. A March 8, 2017 memorandum from United States Attorney General Jeff Sessions says that violent crime will be a priority for the United States Department of Justice.[29] At least one commentator believes that in a time of shrinking budgets, a focus on violent crime means a shift away from white-collar crime.[30] However, as James Connelly of Womble Carlyle in Atlanta has pointed out, federal policies change slowly.[31] Yates herself believes that the priorities laid out in her memorandum represent core values of criminal justice and are thus not ideological.[32] For the purposes of this Article, we will assume that the Yates Memo is indicative of a long-term trend in federal prosecution.

Similarly, the federal government has become aggressive in pursuing individual wrongdoing in the anti-money laundering ("AML") sector. In *Treasury v. Haider*, Civil No. 14-CV-9987 (S.D.N.Y.), the United States Attorney's Office for the Southern District of New York (acting on behalf of FinCEN at the United States Department of Treasury) issued a 146-page complaint against MoneyGram International's former Chief Compliance Officer, Timothy Haider, for the willful failure to implement an effective

---

[28] Yates Memo, https://www.justice.gov/archives/dag/file/769036/download.

[29] Memorandum, *available at* http://apps.washingtonpost.com/g/documents/world/read-the-memo-sent-by-sessions-on-violent-offenders/2367/.

[30] Bethany McLean, *Why White-Collar Crooks May Be Cheering This Sessions Memo*, YAHOO (Mar. 21, 2017), http://finance.yahoo.com/news/why-white-collar-crooks-may-be-cheering-this-jeff-sessions-memo-133115487.html.

[31] James Connelly, *Trump Administration Likely to Maintain Yates Memo Priorities on Corporate Wrongdoing*, WOMBLE CARLYLE (Feb. 14, 2017), http://www.wcsr.com/Insights/Articles/2017/February/Trump-Administration-Likely-to-Maintain-Yates-Memo-Priorities-on-Corporate-Wrongdoing?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[32] *Id.*

AML compliance program or properly file suspicious activity reports, as required under the Bank Secrecy Act.[33] The acts in that case occurred in New York, among other places. Haider allegedly failed to implement disciplinary or termination policies, contravening legal advice provided to Haider.[34] Despite the fact that Haider had knowledge of the fraudulent activity occurring at MoneyGram by its agents and outlets, he continued to allow those agents and outlets to conduct the fraud through MoneyGram's currency transfer system.[35] The complaint also alleges that Haider knew or should have known specific agents posed an unreasonable fraud risk, which MoneyGram's Director of AML Compliance called "egregious and beyond anyone's ability to doubt that the agent and knowledge and involvement."[36] Nevertheless, Haider did not cut ties with any agents or outlets.[37] Finally, while Haider was in charge SAR analysts were unable to access sufficient information to file SARS because Haider kept each department in a separate "silo."[38] Because of this, they failed to have a coherent diligence process, and ignored warning signs regarding authorizing new agents or outlets.[39] Even though the case is still ongoing, the thoroughness of the complaint, the magnitude of the violations, and the District of Minnesota's denial of Mr. Haider's claim that only financial institutions themselves are liable for the failure to maintain an effective AML program, could all be harbingers of the future.[40]

In terms of individual liability, in New York, "[a] person is criminally liable for conduct constituting an offense which he performs or causes to be performed in the name of or in behalf of a corporation to the same extent as if such conduct were performed in his own name or behalf."[41] Although this statute appears to lack a

---

[33] *FinCEN Seeks Civil Money Penalty and Injunction Against Former Chief Compilance Officer of MoneyGram*, FINCEN (Jan. 2, 2015), http://www.sidley.com /en/news/2015-02_banking_and_financial_services_update (citations omitted).

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *See generally* Gonzalez & Carey, *supra* note 27.

[41] N.Y. PENAL LAW § 20.25 (2016).

mens rea requirement, New York adopts the Model Penal Code's definitions for "purposely," "knowingly," "willfully," "recklessly," and "negligently."[42] When a *mens rea* requirement is not stated in a criminal statute, the intent is nevertheless established if the defendant acted purposely, knowingly, or recklessly.[43] Thus, corporate criminal liability arises when an individual commits an offense purposely, knowingly, or recklessly. It is unclear whether the New York Attorney General ("NYAG") is prioritizing individual corporate liability, as their counterparts in Washington, D.C. are, but given the language of New York's final rules, described *infra*, as well as New York's reputation as the financial center of the United States, the NYAG is likely to follow suit.

The individual liability is strongest in the cybersecurity rules, so our discussion will begin there.

B. Cyber-Attacks

Cyber-attacks – "an attack initiated from a computer against a website, computer system or individual computer . . . that compromises the confidentiality, integrity or availability of the computer or information stored on it"[44] - are not new.[45] Cyber-attacks take many forms, including: gaining or attempting to gain unauthorized access to a computer system; denial of service attacks; installation of viruses; and unauthorized use of a computer for processing or storing data.[46] The first cyber-attack occurred in 1988 when Robert Tapan Morris – a professor who now works at MIT that was convicted for the cyber-attack – introduced the Morris

---

[42] N.Y. PENAL LAW § 15.05 (2016).

[43] *See generally* the Model Penal Code.

[44] VINCE FARHAT, BRIDGET MCCARTHY, & RICHARD RAYSMAN, HOLLAND & KNIGHT, CYBER ATTACKS: PREVENTION AND PROACTIVE RESPONSES (2011), *available at* https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/Cyber-attacksPreventionandProactiveResponses.pdf.

[45] NATO, *The history of cyber attacks – a timeline*, *available at* http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

[46] Farhat, McCarthy, and Raysman, *supra* note 44.

worm to determine the size of the Internet.[47] The worm replicated itself to multiple computers through weaknesses in the UNIX system, and slowed down those computers to the point that they were unusable.[48]

At first, the most serious cyber-attacks seemed to focus on government and military servers. For example, in the 2000s, countries as diverse as China, Estonia, and the United States reported hacks on various government servers, as well as hacks on private email servers belonging to high-ranking officials.[49] Nevertheless, by 2010 cyber-attacks on private websites had become a frequent occurrence. To illustrate, throughout December of 2009 and January of 2010 a group calling itself the "Iranian Cyber Army" disrupted both Twitter and the Chinese search engine Baidu to redirect users to a site containing a political slogan.[50] In 2013, some South Korean financial institutions reported a cyber infection resembling past cyber efforts by North Korea.[51]

Indeed, as connectivity throughout the world has increased over the last seventeen years, so too has cyber-attacks.[52] In 2007, the U.S. Computer Emergency Readiness Team, an arm of the Department of Homeland Security ("DHS"), reported 12,000 cyber-incidents. Because DHS defines a cyber-incident as a "violation of an explicit or implied security policy," and provides examples such as denials of service, the unauthorized use of a system for processing or storing data, and attempts to gain unauthorized access to systems or their data,[53] we may infer that cyber-incidents and cyber-attacks are functionally similar, if not identical. By 2009, the number of cyber-incidents had doubled from 2007; in 2012, the number had

---

[47] NATO, *supra* note 45.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] Brian Fung, *How Many Cyberattacks Hit the United States Last Year?*, NEXTGOV (Mar. 8, 2013) http://www.nextgov.com/security/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.

[53] Press Release, Department of Homeland and Security, *Report Cyber Incidents*, DEP'T OF HOMELAND SECURITY, *available at* https://www.dhs.gov/how-do-i/report-cyber-incidents (last accessed Nov. 30, 2016).

quadrupled. It is unclear whether this result occurred due to an increase in attacks, or due to an increase in detection. Regardless, the number of attacks underlines the frequency of cyber-attacks.

Cyber-attacks can have many effects depending on what specific entity is attacked, and the level of the breach. For example, energy company BP reports 50,000 attempted cyber-attacks per day.[54] These intrusions can range from something as harmless (albeit annoying) as taking down the website to keep web browsers from learning more about the company, to a highly-damaging intrusion that steals long-term strategy, confidential project-related employee emails, or proprietary information regarding a company's manufacturing process. The National Nuclear Security Administration, an agency tasked with the military application of nuclear science, records 10 *million* hacks a day.[55] Given that the National Nuclear Security Administration handles nuclear security for the United States and assists the military in determining the effectiveness of nuclear weapons,[56] a successful cyber-attack on this organization could be disastrous to international security.

Financial institutions can suffer greatly from a cyber-attack. For example, in June of 2016 the international consulting firm Deloitte published a report outlining 14 business impacts of a cyber-incident.[57]

---

[54] Michael Tomaso, *BP Fights Off Up to 50,000 Cyber-Attacks a Day: CEO*, CNBC.Com (Mar. 6, 2013), *available at* http://www.cnbc.com/id/100529483.

[55] Jason Koebler, *U.S. Nukes Face Up to 10 Million Cyber Attacks Daily*, U.S. NEWS & WORLD REPORT (Mar. 20, 2012), http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

[56] *Our Mission*, NAT'L NUCLEAR SECURITY ADMIN, https://nnsa.energy.gov/ourmission.

[57] *See* Deloitte, Press Release (June 15, 2016)(listing customer breach notifications; post-breach customer protection; regulatory compliance; public relations/crisis communications; attorney fees and litigation; cybersecurity improvements; technical investigations; insurance premium increases; increased cost for debt raising; operational disruption or destruction; lost value of customer relationships; lost contract revenue; devaluation of trade name; and loss of intellectual property).

C. Money Laundering

"Simply put, money laundering is the process of making dirty money look clean."[58] That is money laundering in a nutshell, but the simplicity of the statement hides the complexity of the crime. For example, money laundering is not just about cash; the Financial Action Task Force ("FATF") has demonstrated "that money laundering can be achieved through virtually every medium, financial institution or business."[59] Though once considered integral only with drug trafficking, money laundering is a necessary step in virtually any criminal activity yielding profits.[60]

Criminals launder money for three reasons. First, it represents the lifeblood of the organization allowing members to cover expenses, maintain inventories, bribe officials, expand illegal enterprises, and finance their lifestyles.[61] Second, it would be foolish to take money directly from these enterprises for those purposes, as law enforcement can easily trace the funds' origin.[62] Third, these criminal proceeds can be the target of investigation and seizure.[63] Consequently, criminals have a high incentive to conceal the existence of these funds or make illegal proceeds appear legitimate to confound law enforcement and continue the criminal enterprise.[64]

Generally, money laundering can be divided into three stages: (1) placement, (2) layering, and (3) integration. Placement, as the first step, is "the physical disposal of cash or other assets derived from criminal activity."[65] The funds can be placed into the financial system, or they can be placed into casinos, shops, and other businesses.[66]

---

[58] Study Guide for the ACAMS Certification Examination 13, ASSOC. OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS, (5th ed. 2015).

[59] *Id.* at 14.

[60] William R. Schroeder, *Money Laundering: A Global Threat and the International Community's Response*, FBI Law Enforcement Bulletin, 1 (FBI, D.C.), (May 2001).

[61] *Id.* at 1.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] Schroeder, *supra* note 60, at 15.

[66] *Id.* at 15.

Layering, the second step, consists of separating illegal proceeds from their source through layers of financial transactions intended to conceal the origin of the proceeds.[67] Layering "involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to disguise the audit trail, source and ownership of funds."[68] The final step of the process is integration. In integration, money is reintroduced into the economy through various methods making it almost impossible for the funds to be traced back to their illicit origin.[69]

Money laundering affects the economy and society in various ways, and while these effects are present in the United States, they tend to be more pronounced in emerging markets.[70] Consequently, emerging markets serve as effective examples when studying the consequences of money laundering. The World Bank has identified five areas where money laundering affects developing countries:

1. Increased crime and corruption;
2. Damaged reputations and international consequences;
3. Weakened financial institutions;
4. Compromised economy and financial sector; and
5. Damaged privatization efforts.[71]

Let's focus on 1, 3, and 4. It should come as no surprise that when a country is viewed as a money-laundering haven, criminals are likely to go there.[72] This in turn generates more crime and

---

[67] *Id.* at 16.

[68] *Id.* at 16.

[69] *Id.* at 18.

[70] John McDowell & Gary Novis, BUREAU OF INT'L NARCOTICS & LAW ENFORCEMENT AFFAIRS, *The Consequences of Money Laundering and Financial Crime*, U.S. Dep't of State 7 (May 2001).

[71] Paul Allen Schott, *Reference Guide to Money Laundering and Combating the Financing of Terrorism,* THE WORLD BANK & INTERNATIONAL MONETARY FUND, Section II at II-1 (2006)[*hereinafter* "The World Bank"].

[72] *Id.* at II-2.

corruption.[73] Finally, it also encourages bribery in functionaries that are critical to the economy, including lawyers.[74]

Financial institutions face unique threats from money laundering because financial transactions can occur instantaneously. Typically, the risks faced by financial institutions due to money laundering can be categorized as reputational, operational, or legal and concentration risks.[75] Reputational risk is defined as the risk that public perception of a bank's business practices and associations, regardless of their accuracy, will cause a decline in the public's confidence in the institution and its integrity.[76] Operational risk is the loss potential from inadequate or failed internal procedures, whether systems-based or human-based.[77] Legal risk is the risk of lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses, or even institution closure.[78] Finally, Concentration risk is the loss potential of a company due to credit or loan exposure to borrowers.[79] For example, when a bank lacks knowledge about a customer, the customer's business, or the customer's status with other creditors, the Bank has concentration risk.[80]

---

[73] *Id.* at II-3.

[74] *Id.* at II-3. Whether lawyers should report a client's suspicious transactions has long been the subject of controversy. *See* AM. BAR ASSOC., STANDING COMM. ON ETHICS & PROF'L RESPONSIBILITY, FORMAL OP. 463, CLIENT DUE DILIGENCE, MONEY LAUNDERING, & TERRORIST FINANCING (May 23, 2013) (providing risk-based control measures to assist lawyers in avoiding aiding illegal activities "consistent with the Model Rules."); Joel Schectman, *U.S. Lawyers Are A Money Laundering Blindspot, Some Argue*, WALL ST. J. (May 11, 2015, 5:30 A.M. ET) (discussing the controversy over whether lawyers in the United States should report suspicious transactions as attorneys must do in the European Union); *See generally* Adam K. Weinstein, *Prosecuting Attorneys for Money Laundering*, 51 DUKE L. J. 371, 372, 378-386 (1988) (arguing that "subjecting attorneys to criminal and civil prosecution violates their clients' right to counsel, right to counsel of choice, and right to effective assistance of counsel.").

[75] The World Bank, *supra* note 71, at II-4.

[76] *Id.* at II-5 (citation omitted).

[77] *Id.* at II-5 (citation omitted).

[78] *Id.* at II-5 (citation omitted).

[79] *Id.* at II-5.

[80] *Id.* at II-5.

Many recent cases highlight the dangers financial institutions face in money laundering. HSBC's recent $1.9 billion settlement with the United States government is a salient example of how money laundering affects financial institutions.[81] HSBC "failed to apply legally required money laundering controls to $200 trillion in wire transfers alone, in only a three year period."[82] In fact, the Bank's inadequacies were so great that the DOJ discouraged HSBC from publicizing the incident to avoid further criminal exploitation of HSBC's compliance gaps.[83]

Money launderers commonly use "front companies," which appear legitimate and engage in legitimate business, but are controlled by criminals.[84] Front companies are not concerned with making a profit; they are concerned with preserving and protecting illegitimate funds.[85] Front companies have access to illicit funds that can be used to subsidize the front company's products and services. As a result, this makes it difficult for legitimate enterprises to compete with those front-companies that need-not rely on the company's actual revenue to continue operations.[86] If a criminal organization gets big enough, the organization can control entire sectors of the economy, which in turn leads to economic instability due to a misallocation of resources from "artificial distortions in asset and commodity prices."[87] Front

---

[81] *See* Heather A. Lowe, *Money Laundering & HSBC – How it affects you*, REUTERS (Jan. 10, 2013, 22:01 GMT) (discussed *supra* and *infra*). HSBC avoided an indictment because state and federal authorities concluded that criminal charges would jeopardize the bank and destabilize the financial system. Ben Protess & Jessica Silver-Greenberg, *HSBC to Pay $1.92 Billion to Settle Charges of Money Laundering*, N.Y. TIMES (Dec. 10, 2012 4:10 P.M.)

[82] *Id.*

[83] James Ball & Harry Davies, *HSBC money-laundering procedures "have flaws too bad to be revealed,"* GUARDIAN (Jun. 5, 2015, 10:10 EDT), http://www.theguardian.com/business/2015/jun/05/hsbc-money-laundering-procedures-flaws-too-bad-to-be-revealed (last visited Nov. 18, 2015).

[84] The World Bank, *supra* note 71, at II-6.

[85] *Id.* at II-6.

[86] *Id.* at II-6.

[87] *Id.* at II-6 (*citing* John McDowell & Gary Novis, Economic Perspectives, U.S. State Dep't, May 2001).

companies can also serve as a tax-evasion vehicle, depriving a country of revenue it would have otherwise received.[88]

In the United States, organized crime has used pizza parlors to launder heroin trafficking proceeds.[89] The "Pizza Connection Trial" lasted from September 30th, 1985 and ended on March 2nd, 1987, making it the longest federal criminal trial in the Southern District of New York at the time.[90] 19 defendants in a Mafia group ranging from Brazil, Sicily, New York and the Midwest were charged in participation of a drug ring trafficking heroin and cocaine, laundering tens of millions of dollars through the use of pizza restaurants as fronts.[91] The case – led by then-federal prosecutor Rudolph Giuliani and involving former-prosecutor Louis B. Freeh– cost millions of dollars to complete.[92] These tens of millions of dollars undoubtedly created the distortions mentioned above, and ultimately 17 of the defendants were found guilty.[93]

In the United States, the methods of money laundering have remained stable for the past ten years.[94] They can be classified as one of the following methods:

---

[88] The World Bank, *supra* note 71, at II-6.

[89] John McDowell & Gary Novis, *The Consequences of Money Laundering and Financial Crime*, ECONOMIC PERSPECTIVES (Dep't of State, D.C.) (May 2001), at 7, http://www.ait.org.tw/infousa/zhtw/DOCS/ijee0501.pdf (last accessed Mar. 26th, 2016).

[90] Ralph Blumenthal, *Acquitted in "Pizza Connection Trial," Man Remains in Prison*, N.Y. Times (Jul. 28, 1988), *available at* http://www.nytimes.com/1988/07/28/nyregion/acquitted-in-pizza-connection-trial-man-remains-in-prison.html.

[91] *Id.*

[92] *Id.*

[93] *Id.* To learn more about the Pizza Connection Trial, *see generally* Shana Alexander, THE PIZZA CONNECTION: LAWYERS, MONEY, DRUGS, MAFIA (1988) (discussing the trial); *see also* John Surico, *How Mafia Pizzeria Drug Fronts Inspired One of the Most Complex Criminal Trials Ever*, VICE (Jan. 28, 2016), http://www.vice.com/read/how-mafia-pizzeria-drug-fronts-inspired-one-of-the-most-complex-criminal-trials-ever ("'It was a trial with no end in sight involving a billion puzzle pieces," said [organized crime expert] David Amoruso . . . "all of its participants – defendants, lawyers, prosecutors, jurors, and the judge - had to do their best not to be driven totally insane.").

[94] *See* U.S. DEP'T OF TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT 3 (2015) ("This assessment finds that the underlying money

1. Use of cash and monetary instruments in amounts under regulatory recordkeeping and reporting thresholds;

2. Opening bank and brokerage accounts using nominees to disguise the identity of the individuals who control the accounts;

3. Creating legal entities without accurate information about the identity of the beneficial owner;

4. Misuse of products and services resulting from deficient compliance with anti-money laundering obligations; and

5. Merchants and financial institutions wittingly facilitating illicit activity.[95]

By reviewing the above methods, one may notice that all five methods relate to financial institutions. These funds derive mainly from fraud and drug trafficking.[96] Fraud covers a wide range of crimes, like healthcare fraud, federal government payments fraud, and identity fraud.[97] Drug trafficking alone generates an estimated $64 billion in cash per year.[98] Furthermore, recent evidence suggests the severance of customer relationships between U.S. banks and Mexican money exchangers, commonly known as "casas de cambio,[99] "has led to increases in the retention and use of drug-related cash, both in the United States and internationally, which has "shifted money laundering activity from Mexico to the United States."[100]

laundering vulnerabilities remain largely the same as those identified in the 2005 United States Money Laundering Threat Assessment.")

[95] *Id.* at 3.

[96] *Id.* at 2.

[97] *Id.* at 2.

[98] *Id.* at 2.

[99] Hannah Stone, *US Targets Bank in Mexican Money Laundering Crackdown*, INSIGHT CRIME, "Exchange houses which are often used by Mexican criminal groups to launder funds." *available at* http://www.insightcrime.org/news-analysis/us-targets-bank-in-mexico-money-laundering-crackdown

[100] *Id.* at 3.

Now, one can also imagine how a criminal, state actor, or non-state actor might try and bypass cyber-security protocols to commit a crime, and then launder the proceeds of the crime. For example, in 2015 a gang of hackers infiltrated more than 100 banks in 30 countries.[101] At the time of the hack, employees were unknowingly opening emails that allowed hackers to insert malware.[102] This malware manipulated the banks' cyber-security protocols and proceeded to and siphon as much as $1 billion directly from the banks over a two-year period.[103] To cover their tracks the hackers layered the proceeds into their own accounts.[104]

A further example can be found in a FINRA report from February 2016 describing an incident where foreign customers considered to be "high-risk" opened four accounts with an online firm and engaged in patterns of fraudulent trading through the firm's Direct Market Access (DMA) platform.[105] These customers hacked other online broker-dealers' accounts, engaging in a short sale schemes that resulted in large profits for the customers' of the firm through their accounts, and losses in the compromised broker-dealer accounts.[106] FINRA punished the online firm for "failing to establish and implement [AML] policies and procedures adequately tailored to the firm's online business in order to detect and cause the reporting of suspicious activity; and . . . failing to establish and implement a reasonably designed customer identification program to adequately verify customer identity."[107]

Curiously, NYDFS has recognized the intersection of AML and cyber-security on prior occasions such as when the agency issued

---

101 Thomas Bock, *The Convergence of Anti-Money Laundering and Bank Security*, K2 Intelligence (Nov. 2015), *available at* https://www.k2intelligence.com/en/insights/thought-leadership/the-convergence-of-anti-money-laundering-and-cyber-security.

102 *Id.*

103 *Id.*

104 *Id.*

105 FINRA, REPORT ON CYBERSECURITY PRACTICES (Feb. 2015), *available at* http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

106 *Id.*

107 *Id.*

its BitLicense regulations.[108] These regulations required financial institutions to have designated compliance personnel and AML procedures that are the same as those for institutions handling traditional, fiat currency.[109]

The United States Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") has also started making the connection between cyber-security breaches and money laundering schemes.[110] FinCEN has recently begun to encourage financial institutions to include information on cyber-security events or breaches on Suspicious Activity Reports ("SARs").[111] Specifically, the guidelines provide guidance for SAR reporting in connection with: cyber-enabled crime and cyber events; the inclusion of relevant cyber-related information in SARs; encouraging collaboration between cybersecurity units and AML units within the same firm; and sharing cyber-related information across financial institutions to combat money laundering, terrorism financing, and cyber-attacks.[112] The efficacy of linking a cybersecurity event to a SAR is evidenced by the Federal Bureau of Investigation's use of a SAR to trace $7 million dollars from a Florida bank account to criminals in Russia and Ukraine that had released a "Zeus" botnet virus to make the fraudulent withdrawal.[113]

The convergence of opinion between government recommendations and consultants in the private sector point to a growing consensus that, while AML and cyber-security practices do not and cannot have complete overlap in their functions, they do have significant overlap in their goals and methods. It would seem that two functions within the same organization with significantly overlapping missions would have similar regulatory liability when

---

[108] *See generally* Bock *supra* note 104.

[109] *Id.*

[110] Chris Kentours, *Cybersecurity and AML: How the Twain Must Meet?*, FINOPS REPORT (Nov. 10, 2016), *available at* http://finops.co/slider/cybersecurity-and-aml-how-the-twain-must-meet/.

[111] *Id.*

[112] *Id; See also* Clifford Chance PDF (internal citations omitted) (Note that the advisory does not change any of the existing laws).

[113] Kentours, *supra* note 112 at *Id.*

managers in those groups fail to fulfill their duties. As we will see in the next section, this is not the case.

III. THE RULE, INDIVIDUAL CORPORATE LIABILITY, AND SUGGESTIONS

In 2013, the NYDFS conducted a survey on cyber-security.[114] 60 community and regional banks, 12 credit unions, and 82 foreign branches and agencies participated in the NYDFS's questionnaire. The questionnaire asked questions about "each participant's information security framework; corporate governance around cyber security; use and frequency of penetration testing and results; budget and costs associated with cyber security; the frequency, nature, cost of, and response to cyber security breaches; and future plans on cyber security."[115] NYDFS also met with "depository institutions and cybersecurity experts . . . to discuss industry trends, concerns, and opportunities for improvement."[116]

NYDFS's findings discussed management of information technology systems; information security frameworks; use of security technologies; penetration testing; budget and costs; corporate governance; cybersecurity incidents and breaches; and planning for the future.[117] Most institutions experienced intrusions, and the larger the institution, the more likely it was to experience malware and phishing attempts.[118]

It was further noted that larger institutions were more likely to experience financial losses after a cyber-attack.[119] These institutions were also reported to be more likely to have a cybersecurity plan

---

[114] Report on Cyber Security in the Banking Sector, N.Y. DEP'T OF FIN. SERVS. (May 2014), *available at* http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

instituted than their smaller counterparts.[120] Recent examples help illustrate this last point. In 2011, more than 300,000 Citibank accounts were compromised in a targeted hack.[121] In 2012, a cyber-attack focused on employee login credentials at Bank of America and Wells Fargo.[122]

An April 2015 update on the NYDFS report focused on third-party security service providers, as well as steps taken to implement the U.S. Commerce Department's National Institute of Standards and Technology.[123] Most of the institutions involved had taken or were taking steps to implement NIST principles, but the application of those principles varied across institutions.[124] Ultimately, the report concluded that banks were taking steps to increase cybersecurity, although progress varied depending on an institution's size and type.[125]

On September 13th, 2016, New York Governor Andrew Cuomo announced "first-in-the-nation" regulations to protect New York financial institutions from cyber-attacks.[126] In his remarks, Governor Cuomo said:

"New York, the financial capital of the world, is leading the nation in taking decisive action to our consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, terrorist networks, and other criminal enterprises. This regulation helps guarantee the financial services

---

120 *Id.*

121 *Banks Likely to Remain Top Cybercrime Targets*, SYMANTEC (last accessed Nov. 30, 2016), *available at* https://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf. *See also,* Press Release, CitiGroup Inc., Updated Information on Recent Compromise to Citi Account Online for Our Customers, (June 15, 2011), *available at* http://citigroup.com/citi/press/2011/110610c.htm.

122 *Id.*

123 Press Release, NYS Department of Financial Services, *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, NYS DEPARTMENT OF FINANCIAL SERVICES, (April 2015), *available at* http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf [*hereinafter* "2015 Report"].

124 *Id.*

125 *Id.*

126 Governor Cuomo Press Release, *supra* note 8.

industry upholds its obligation to protect consumers and ensure that its systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible."[127]

The proposed regulation includes proposals designed to balance "certain regulatory minimum standards while maintaining flexibility so that the final rule does not limit industry innovation and instead encourages firms to keep pace with technological advances."[128] Although this article is not intended to provide a thorough analysis of the components contained within either the cyber-security rule, or the AML rule, a brief overview nonetheless provides helpful context in regards to the certification rules.

The cybersecurity program requires every covered entity[129] to establish and maintain a cybersecurity program to ensure confidentiality, integrity, and the availability of its Information Systems,[130] which, among other things, means "a discrete set of electronic information resources organized for the collection, maintenance, use, sharing, dissemination or disposition of electronic information."[131] Covered entities are to implement and maintain a written cybersecurity policy setting forth policies and procedures in order to protect Information Systems and private information stored on those systems. The minimum policy standards require covered entities to address:

1. Information security;

2. Data governance and classification;

3. Access controls and identity management;

---

127 *Id.*

128 *Id.*

129 "[A]ny [individual, partnership, corporation, association, or other entity] operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law, or the financial services law."

130 Press Release, Proposed Regulations: Section 500.00, N.Y. DEP'T FIN. SERVS. (September 2016), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf(last accessed Sept. 2016).

131 *Id.*

4. Business continuity and disaster recovery planning and resources;

5. Capacity and performance planning;

6. Systems operations and availability concerns;

7. Systems and network security;

8. Systems and network monitoring;

9. Systems and application development and quality assurance;

10. Physical security and environmental controls;

11. Customer data privacy;

12. Vendor and third-party service provider management;

13. Risk assessment; and

14. Incident response.[132]

This requires the board of directors or an equivalent governing body to review the policy as frequently as necessary (but no less frequently than annually), and a senior officer to approve of the policy's contents.[133]

The proposed regulation also contained an annual certification of compliance requirement.[134] Every covered entity[135] must certify that it follows the requirements of the regulation.[136] The

---

[132] *Id.*

[133] *Id.*

[134] Press Release, Maria T. Vullo, Notice of Final Regulations' Promulgation under Part 500 Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York: Cybersecurity Requirements for Financial Services Companies, 500.17(b), (Feb. 13, 2017), *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[135] *Id.*

[136] *Id.*

language of the certification is found in Appendix A and reads as follows:

> The Board of Directors or a Senior Officer of the Covered Entity certifies:
>
> (1) The Board of Directors (or name of Senior Officer(s)) have reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;
>
> To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity as of ___ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended ____ (year for which Board Resolution or Compliance Finding is provided) complies with Part __.
>
> Signed [and dated] by the Chairperson of the Board of Directors or Senior Officer(s).
>
> Failure to certify will be enforced under "any applicable laws," including civil and criminal penalties.[137]

NYDFS's final cybersecurity regulations went into effect March 1st, 2017.[138] In a February 16, 2017 press release, New York Governor Andrew M. Cuomo said:

---

[137] *Id.*; *see also* PwC, *AML monitoring: New York regulator gets prescriptive*, FINANCIAL CRIMES OBSERVER PWC, (July 2016), *available at* http://www.pwc.com/us/en/financial-services/financial-crimes/publications/assets/aml-monitoring-nydfs-2016.pdf [*hereinafter* "PwC"].

[138] Press Release, Governor Cuomo, Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1, (February 16, 2017), *available at* http://www.dfs.ny.gov/about/press/pr1702161.htm.

> New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks . . . These strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes.[139]

The final regulation includes

- Controls relating to the governance framework for a robust cybersecurity program including requirements for a program that is adequately funded and staffed, overseen by qualified management, and reported on periodically to the most senior governing body of the organization;

- Risk-based minimum standards for technology systems including access controls, data protection including encryption, and penetration testing;

- Required minimum standards to help address any cyber breaches including an incident response plan, preservation of data to respond to such breaches, and notice to DFS of material events; and

- Accountability by requiring identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance to DFS.[140]

Section 500.20, which covers enforcement, says that "This regulation will be enforced by the superintendent pursuant to, and is

139 *Id.*
140 *Id.*

not intended to limit, the superintendent's authority under any applicable laws."[141]

So far - so good. However, in June 2016, NYDFS had issued a similar final rule regarding AML compliance certification.[142] This issuance was a result of multiple NYDFS investigations into compliance at "regulated institutions" ("all banks, trust companies, private bankers, savings banks and savings and loans associations chartered under New York Banking Law, New York-licensed branches and agencies of foreign banking corporations, as well as New York-licensed check cashiers and money transmitters[]"[143]) with applicable money laundering rules.[144] The investigation identified shortcomings in these financial institution's transaction monitoring and filtering programs, which was in turn attributable to a lack of governance, oversight, and accountability at senior levels.[145] Based on this investigation and other factors, NYDFS believed financial institutions had systemic shortcomings in their AML programs and wanted to not only clarify AML program requirements, but also have the Board of Directors or a Senior Officer submit a Board Resolution or Compliance Finding.[146]

The final AML rules require every regulated institution to maintain a Transaction Monitoring Program that should contain, where applicable, the following attributes:

1. Based on the institution's Risk Assessment;

---

141 *Supra* note 10.

142 Publication, Shearman & Sterling LLP, *NYS Department of Financial Services Outlines Requirements for Transaction Monitoring and Filtering Programs of NY State-Licensed Institutions*, SHEARMAN & STERLING LLP CLIENT PUBLICATIONS (Jul. 20, 2016), *available at* http://www.shearman.com/~/media/Files/NewsInsights/Publications/2016/07/NYS-Department-of-Financial-Services-Outlines-Requirements-FIAFR-072016.pdf [*hereinafter* "Shearman and Sterling"].

143 *Id.*

144 *Id.*

145 *Id.*

146 *Id.*

2. Periodically reviewed and updated to reflect and account for changes to BSA/AML laws and other relevant information;

3. Match BSA/AML risks to the firm's business, product and service lines, and customers;

4. BSA/AML detection scenarios with values and amounts that detect potential money laundering, suspicious activity, or other illegal activity;

5. A full scope testing of the Transaction Monitoring Program, including governance review, data mapping, transaction coding, detection scenario logic, model validation, data input and Program output;

6. Documentation articulating the institution's current detection scenarios and the assumptions, thresholds, and parameters of those scenarios;

7. Protocols outlining how the firm will investigate the Transaction Monitoring Program's alerts, how the Regulated Institution will decide which alerts will result in a filing or other action, who is responsible for deciding, and how the investigative and decision-making process is to be documented; and

8. Be subject to on-going analysis in order to determine whether detection scenarios, underlying rules, threshold values, parameters, and assumptions are still relevant.[147]

The Regulated Institution's Filtering Program's requirements are similar to the Monitoring Program in that they are only to be implemented where applicable, and are as follows:

1. Be based on the institution's Risk Assessment;

147 *Id.*

2. Be based on technology, processes, or tools that will match names and accounts consistent with the institution's risks, transaction, and product profiles;

3. Full scope testing of the Filtering Program, including relevant reviews of data matching, determining whether the OFAC sanctions list and threshold settings synchronize to an institution's risks; assessing the logical fit of technology or tools, model validation, and data input with the Program's output;

4. On-going analysis to assess technology and tool's logic and performance in matching names and accounts, as well as the OFAC sanctions list and threshold settings to see if they map the institution's risks, and

5. Documentation articulating the Filtering Program's intent and design for tools, processes, and technology.[148]

Both the Transaction Monitoring and Filtering Programs are required to have, where applicable:

1. ID of all data sources with relevant data;

2. Validation of data's accuracy, integrity, and quality, ensuring accurate and complete data flows through the Transaction Monitoring and Filtering Program;

3. Processes for data extraction and loading to ensure a complete and accurate data transfer from source to system (provided automated systems are used)

4. Governance and management oversight, including policies and procedures that govern changes to the Transaction Monitoring and Filtering Program ensuring that changes are managed, reported, audited, defined, and controlled;

---

[148] *Id.*

5. Vendor selection processes where third-party vendors are used in the Transaction Monitoring and Filtering Program;

6. Funding for the Transaction Monitoring and Filtering Program;

7. Qualified personnel or third-party consultants responsible for various aspects of the Transaction Monitoring and Filtering Program, including design, implementation, ongoing analysis, planning, operation testing, and

8. Periodic training of all Transaction Monitoring and Filtering Program stakeholders.[149]

When Regulated Institutions identify areas, systems, or processes needing material improvements, updates, or redesigns, the Regulated Institutions are required to document the identifications made, and the corresponding planned remedial efforts. The Superintendent of NYDFS must be able to view these documents.[150]

Either the board or the senior officers of a company must certify that the company has followed these rules outlined above. The Board Resolution or Compliance Finding requirement dictates that:

> [E]ach Regulated Institution "shall adopt and submit to the Superintendent a Board Resolution or Senior Officer(s) Compliance Finding in the form set forth in Attachment A by April 15th of each year. Each Regulated Institution shall maintain for examination by the Department all records, schedules and data supporting adoption of the Board Resolution or

[149] *Id.*
[150] *Id.*

> Senior Officer(s) Compliance Finding for a period of five years.[151]

The language of the aforementioned certification is as follows:

> The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary to adopt this Board Resolution or Senior Officer Compliance Finding.
>
> The Board of Directors or Senior Officer(s) has taken all steps necessary to confirm that (name of Regulated Institution) as of ___ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended ___ (year for which Board Resolution or Compliance Finding is provided) complies with [Transaction Monitoring and Filtering Requirements].
>
> Signed [and dated] by each member of the Board of Directors or Senior Officer(s).[152]

In the final rule, these requirements are to "be enforced pursuant to, and is not intended to limit, the Superintendent's authority under any applicable laws."[153] Thus, the scope of the Superintendent's authority is both civil and criminal. However, the original wording of the rule was harsh, as illustrated below:

> All Regulated Institutions shall be subject to all applicable penalties provided for by the Banking Law and the Financial Services Law for failure to maintain a Transaction Monitoring Program, or a Watch List

---

[151] *Id.*

[152] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R. Part 504 (Mar. 2017), *available at* http://docs.dos.ny.gov/info/register/2016/july20/pdf/rulemaking.pdf *and* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf.

[153] Shearman and Sterling, *supra* note 142.

> Filtering Program complying with the requirements of this Part and or failure to file the Certifications required under Section 504.4 hereof. A Certifying Senior Officer who files an incorrect or false Annual Certification also may be subject to criminal penalties for such filing.[154]

It is unclear why the original language was worded as it was. More than likely, the language intended to serve two purposes: (1) to underline the seriousness of the offense, and (2) to warn potential officers certifying the Annual Certification of the consequences resulting from a failure to certify the company's program.

Regardless, due to industry feedback that language was struck out entirely and replaced with new language for the finalized rule. In the final rule, NYDFS removed the threat of criminal penalties for incorrect or falsified filings.[155]

Thus, there are meaningful distinctions between the requirements of the cybersecurity rule and the AML rule. However, the reality of modern financial institutions means that AML is a significant component of cybersecurity, such that AML measures cannot be effective without cybersecurity, and cybersecurity in financial institutions cannot be fully effective without AML measures. In the following section, I will explain why the current rules require some form of harmonization in their application and enforcement, and further, why those rules need to establish a specific standard for the imposition of criminal liability in specific instances.

IV. SUGGESTIONS AND RATIONALE

Both the cybersecurity rules and the AML rules should have the same language, however, they do not. Unfortunately, both rules lack much-needed language allowing for the imposition of criminal liability in appropriate situations. This problem could be addressed

---

154 *Id.*

155 PwC, *supra* note 137.

through a number of ways and considerations. First, one must consider that by softening the language in both rules, the NYDFS was not responsive to institutions' vocalized concerns, and likely only further confused individuals trying to comply. Second, if both rules contain the same language, the possibility of corporate directors avoiding liability in one function, while negating liability in another for the same act, will likely lessen. Third, by emphasizing the potential of corporate criminal liability the rule will more properly reflect the principles outlined by the Yates memorandum. Even though the Yates memorandum is not an official policy of the New York Attorney General's Office, aligning the language of the rules with the spirit of the Yates memorandum could eliminate the complexity created by the current compliance rules for company directors.

A. Changing the Language of the Statute but not the Underlying Enforcement Mechanism is Unresponsive to Concerns and Only Confuses Firms Trying to Comply with the Rule

In response to public comments regarding the rule, the NYSFDS changed the AML rule's language so that the regulation "[would] be enforced pursuant to, and [] not intended to limit, the Superintendent's authority under any applicable laws."[156] Although the laws are not explicitly mentioned, the language of the AML rule presumably refers to legislation relating to Banking, Insurance, and Financial law. However, if this is true, the NYSFDS is committing two errors.

First, by not changing the underlying penalties of the law, the NYSFDS is not being responsive enough to the concerns of commenters. Secondly, by stating only that regulators will pursue enforcement under "any and all applicable laws," individuals are left "in the dark" about specific applicable law. If we were to assume that a law's ability to be interpreted directly influences the law's likelihood of being followed, then one must also consider the vagueness of this rule and its resultant effect on compliance.

---

156 Shearman and Sterling, *supra* note 142.

This problem of vagueness in compliance can also be found in the proposed cybersecurity rule. Like the AML rule, the cybersecurity rule only states that the Superintendent will enforce the Regulation pursuant to "authority under any applicable laws."[157] One can only speculate why the rule is phrased this way. Perhaps this phraseology was a response to the public comment regarding the AML rules and was intended to preemptively address similar complaints about the AML rule. Again, however, this language is ineffective at best and counterproductive at worst. This lack of clarity could feasibly hinder corporations from ensuring which laws are applicable, and consequently, what standards to adhere to when certifying their cybersecurity programs.

Furthermore, rule-makers determined that the prior language was not precise enough to warrant inclusion. As we have seen, cybersecurity breaches and AML risks are frequent. Thus, this arguably makes individual penalization through criminal liability unjust in certain situations, such as, for example, the filing of false or incorrect Annual Certifications in good faith. Beyond that, a variety of scenarios could occur: firms may have to start offering large salaries to compliance officers just to attract quality talent, or, firms may feel encouraged to structure their company in such a way that does not require a New York state business charter, and thus bypassing the rule. In a true nightmare scenario, firms could just dissolve their charters, leave New York, and set up shop in alternative financial centers such as San Francisco, Boston, Chicago, Charlotte, or Washington, D.C.

B. Uniform Language as a Response to Dual Corporate Officer Liability Loopholes

As the rules are currently written, it is entirely possible that an individual could face criminal liability for a certification violation in the cybersecurity context, yet simultaneously avoid criminal liability under the AML rules. To be sure, in some situations this will not be relevant. For example, suppose that there is a cybersecurity breach of

---

157 Vullo, *supra* note 134.

a financial institution based on corporate espionage. If, after an individual makes a bad faith cybersecurity certification, a hacker gets into an employee's email, he may learn of a new marketing campaign, the valuation of a confidential M&A deal, or proprietary research created by a firm's research team. Cybersecurity breaches involving financial institutions are often related to some form of money laundering activity. Such breaches are cybersecurity breaches, although they do not involve the laundering of money.

However, in situations where a cybersecurity breach does involve money laundering, if both the cybersecurity policy and money laundering policy were certified by an individual omission or outright lie, it is possible that the individual could avoid liability under the AML rule, but not the cybersecurity rule. A predictable argument could be that criminal prosecution under the AML rule is unfair because the language change from the proposed rule to the final rule reflects a retraction in the intended harshness of the policy against criminal prosecution. Thus, it is foreseeable that criminal liability was not intended to be permissible for AML violations, and the rule is thus arguably be unconstitutional for being overly vague.

However, if both rules were to have the exact same language, two results would occur. First, loopholes are no longer present in those situations where both rules apply, but with contrasting language. Second, assuming all elements are met, it would be difficult, if not impossible, for an individual to argue that it was unclear whether their failure to comply with the certification mechanism would allow for criminal liability sanctions.

C. The Yates Memorandum & Creating a Comprehensive Model

Having a rule that reflects the Yates memorandum not only makes the rule easier to follow, but also sets good precedent for further states' adoption and implementation. Responding to industry concerns, eliminating the possibility of loopholes, and creating precise language are key aspects of the new language. The next and final element is that the new language should reflect the tenor of the Yates memorandum, such that it makes the rule easier to follow, but

also sets a good precedent for other states to copy should they choose to implement their own state policies.

Again, it bears repeating that the Yates memorandum, technically, has no bearing on the New York Attorney General's Office or the NYDFS. After all, the Yates memorandum is part of the DOJ, and thus reflects federal policy. However, many New York banks have not worked solely within the confines of New York for quite some time: indeed, it is hard to recall when New York banks operated solely within the United States. Goldman Sachs, JPMorgan and Deutsche Bank are just a few New York chartered organizations with international reach.[158] As such, in their operations these institutions are subject to not just New York law, but federal law as well. Despite New York's outsized influence within the financial sector, common practice for these organizations is to channel their resources towards federal law compliance.

There is another advantage to this. By making the rule reflective of the Yates memorandum and easier to follow, it removes an incentive for an organization to move its banking charter from New York to another state with more relaxed banking standards.

V. THE NEW RULE

If the current language and the proposed language of both the cybersecurity and AML certification policies are not adequate, then what is? This author proposes the following rules for the cybersecurity and AML programs, respectively. For cybersecurity:

All Regulated Institutions shall be subject to all applicable penalties provided for by the Banking Law and the Financial Services Law for failure to maintain a cybersecurity program complying with the requirements of this Part and or failure to file the Certifications required under Section 500.17 hereof. A Certifying Senior Officer

[158] *See generally* Report, New York State Chartered Institutions as of December 31, 2012, N.Y. DEP'T FIN. SERVS. (Dec. 31, 2012), *available at* http://www.dfs.ny.gov/reportpub/annual/annualbanklist.htm.

who *intentionally*, *knowingly*, or *recklessly* files an incorrect or false Annual Certification also may be subject to criminal penalties for such filing.

Then, for the AML:

All Regulated Institutions shall be subject to all applicable penalties provided for by the Banking Law and the Financial Services Law for failure to maintain a Transaction Monitoring Program, or a Watch List Filtering Program complying with the requirements of this Part and or failure to file the Certifications required under Section 504.4 hereof. A Certifying Senior Officer who *intentionally*, *knowingly*, or *recklessly* files an incorrect or false Annual Certification also may be subject to criminal penalties for such filing.

This proposed language achieves two purposes. First, by giving explicit standards, the language makes clear that a criminal enforcement will only be triggered where an individual's behavior manifests a level of intent beyond mere negligence. The *Haider* case, described *supra*, provides a clear example of when an individual director's failure to provide adequate internal controls was a result of mere negligence. As illustrated by the *Haider* case, it would be unfair to punish all individuals for negligence or strict liability offenses and could lead to unintended consequences in an industry where complete prevention has proven impossible. Second, and relatedly, this proposed rule reflects the reality that AML and cybersecurity divisions at certain financial institutions face extraordinary difficulties and overlapping functions. The proposed rule is narrowly tailored to prevent the behavior seen in *Haider*, or rather, violations conducted by individuals intentionally, knowingly, or recklessly; but not the behavior of otherwise good-faith individuals who mistakenly certify a compliance program. Distinguishing between negligent and reckless conduct may be difficult at times, but nonetheless, this proposed rule provides a minimum standard and guide for enforcement agencies to adhere to.

VI. CONCLUSION

AML and cybersecurity are separate policies, yet, closely intertwined and critical as a defense for financial institutions. These institutions are constantly under attack from outsiders, and unfortunately, bound to fall victim to a breach at some point. After all, even if 10,000 attacks occur and 9,999 of them fail, all it takes is one; hackers may still be successful in damaging a targeted institution, even when the breach is minimally intrusive.

The New York State Department of Financial Services made a mistake in weakening the language of its proposed rules. The NYDFS was not responsive to industry concerns and the rules were not written clearly enough to meaningfully advise parties affected by the consequences of a failure to comply. By strengthening the language so that clear consequences are understood and established, and by setting a clear standard of what will trigger potential criminal liability, this Author's proposed language will serve the dual purpose of reassuring individuals at firms of what actions would impose criminal liability, and would further ensure the New York State Department of Financial Services that its goal of increasing cybersecurity and AML regulations has been met.